DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Firewalls

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Checkpoint Firewall Juniper Cisco PIX Firewall Nokia 120, Nokia IP 330 appliance Fiber link Firewall Firewall-MS ISA and Zone Alarm WatchGuard Firebox II Border Manager (Novell & MS) McAfee Firewall 4.0 G2, XP Firewall, BlackIce		Firewall with enhanced deep packet inspection. Deperimeterization requires defense in layers strategy.
		Shared ✓ **Agency** ✓

Retirement Targets

Mainstream Platforms

Juniper, Cisco PIX, Checkpoint

Containment Targets

Contain everything else with one footnote (see below)

Emerging Platforms

Enhanced deep packet inspection & evolving multipurpose security w/ increased functionality.

Implications and Dependencies

Deep packet inspection (DPI) is viewed as a must have feature because of the increasing blended attacks even in the tactical deployment. Perimeter firewalls that do not have DPI or limited DPI should be augmented with an intrusion prevention device.

Roadmap Notes

- Nokia H/W appliance running Checkpoint is valid for implementation.
- The committee plans to review this discipline yearly during August.

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Firewalls

- **Discipline Boundaries:**
  - While separate disciplines, desktop firewalls and perimeter firewalls are not mutually exclusive of one another. The best implementation strategy would be a layered approach with a strong perimeter defense supplemented by a strong desktop defense. In many instances, you would model the firewall strategy after the evolution of the anti-virus strategy with at least a clear two tier approach. In some cases, additional firewalls or IPS implementations would be necessary to protect extremely sensitive data from both internal and external threats and to provide a third tier. Each implementation is situational with at least a deep packet inspection (DPI) perimeter solution.

- **Discipline Standards:**

- **Migration Considerations:**
  - Should an agency convert to a recommended firewall products, expect a price of $5K to $15K. This is the current price with deep packet inspection and VPN capabilities with four 10/100 network connections.

- **Exception Considerations:**

- **Miscellaneous Notes:**

- **Established Date**
  - April 28, 2004

- **Date Last Updated:**
  - August 23, 2006

- **Next Review Date:**
  - August 2007